SEGURINFO 2015

LIII Congreso y Feria Iberoamericana de Seguridad de la Información

USUARIA

Protección de Infraestructuras Críticas
Seguridad en Sistemas de Control Industrial

Presentada por:

Julio César Ardita, CTO CYBSEC

jardita@cybsec.com

21 de mayo de 2015

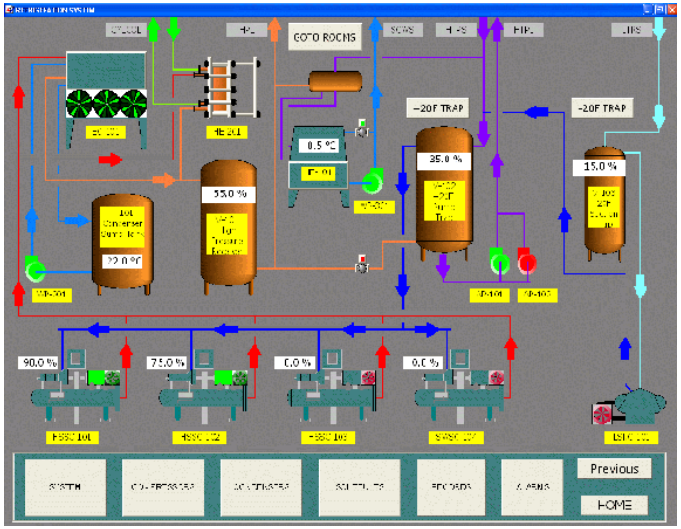
Aclaración:

© Todos los derechos reservados. No está permitida la reproducción parcial o total del material de esta sesión, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares de los derechos. Si bien este Congreso ha sido concebido para difusión y promoción en el ámbito de la profesión a nivel internacional, previamente deberá solicitarse una autorización por escrito y mediar la debida aprobación para su uso.

Agenda

- Introducción a los ICS
- Riesgos actuales
- Estrategias de Seguridad
- Estándares y lineamientos de seguridad

Introducción a los ICS



Alcance de las Infraestructuras críticas

- Administración
- Espacio
- Industria Nuclear
- Industria Química
- Instalaciones de Investigación
- Agua
- Energía
- Salud
- Tecnologías de la Información y las Comunicaciones (TIC)
- Transporte
- Alimentación
- Sistema Financiero y Tributario

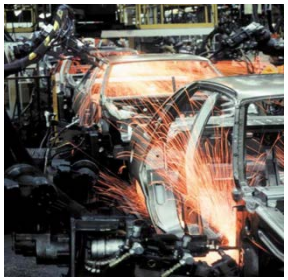
Tipos de Industrial Control Systems (ICS)

Supervisory Control And Data Acquisition (SCADA)

Process Control Systems (PCS)

Distributed Control Systems (DCS)

Automation



Situación actual

- Organizaciones públicas y compañías privadas.

- No existen regulaciones relacionadas con la seguridad de la información de los sistemas de infraestructuras críticas.

- En las Organizaciones, el sinónimo es protección de redes SCADA.

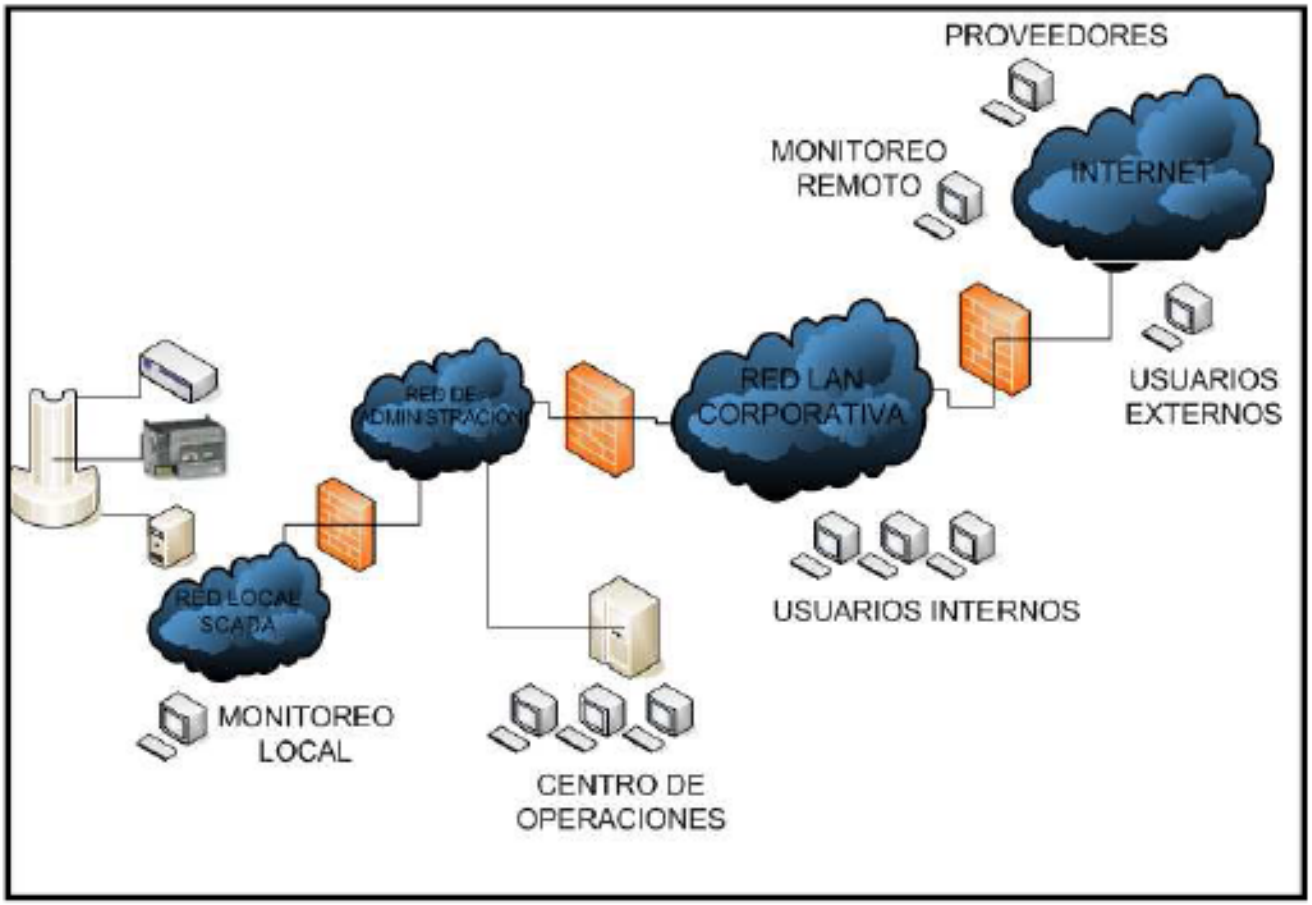
La red SCADA era/es manejada por ingenieros y proveedores.

Seguridad Corporativa se está metiendo en el tema.

- Integración con la red corporativa
- Aplicación de estándares
- Actualización / Patches

Situación actual

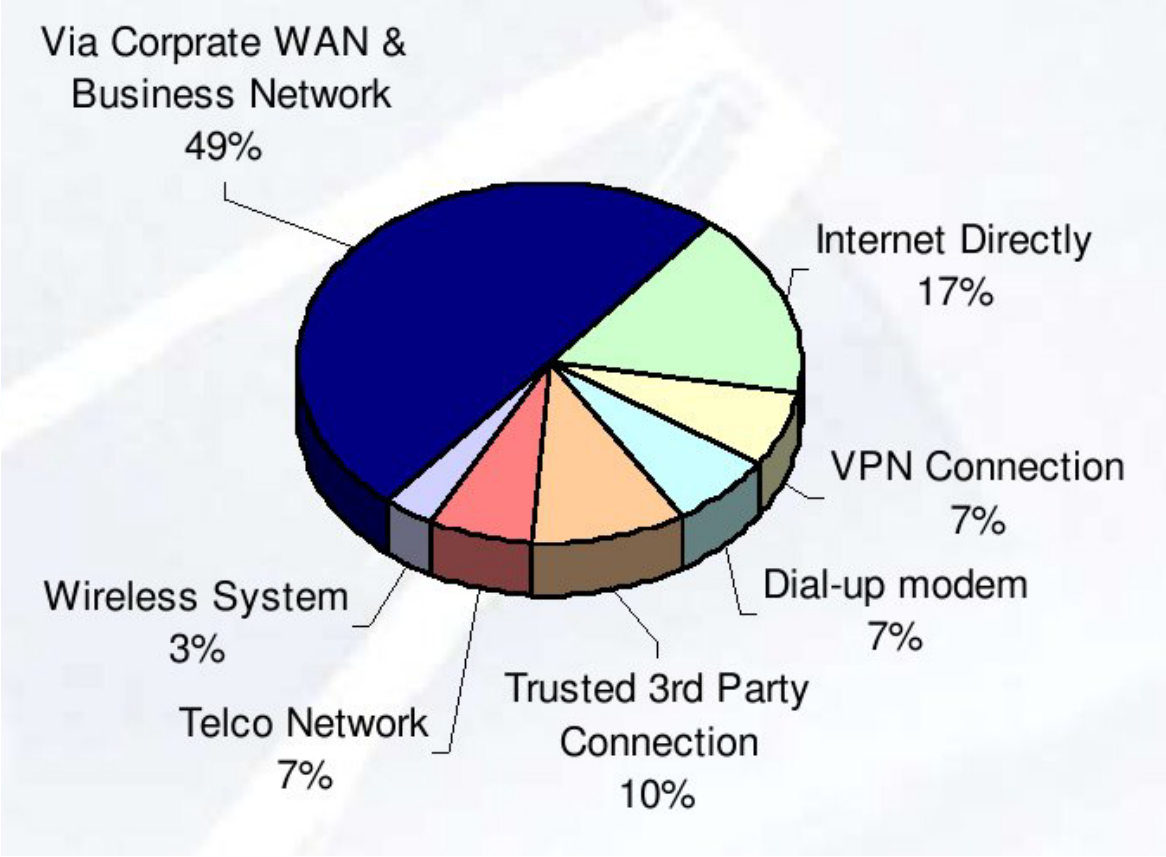
Modelo de interconexión



Riesgos actuales

Scan Results
Scan Thread 1 (http://www.scanme.com:80/acublog)
Web Alerts (116)
SQL Injection (AS) (12)
Cross Site Scripting (22)
/acublog/comments.aspx (22)
tbComment (22)
Blind SQL/XPath injection (6)
Cross Frame Scripting (2)
User credentials are sent in clear text (4)
SMB null session (1)
ASP.NET debugging enabled (13)
Directory listing found (1)
Password type input with autocomplete enabled (4)

Vectores de ataque en ICS



Intrusiones a ICS

Popular Mechanics

http://www.popularmechanics.com/technology/military/4307528

How Hackers Could Take Down a Natural Gas Pipeline

Much of America's infrastructure is computer-controlled, and therefore subject to hacking. It's a subject we take on in depth in our April cover story about preventing cyber attacks on U.S. soil. Here is an in-depth look at the specific vulnerabilities of a natural gas pipeline, and a status check on the security of five key sectors of U.S. infrastructure.

BY GLENN DERENE

FLASH-DRIVE DROP

Where: Parking Lot
Human nature can sometimes provide an easy end run around a strong firewall. An old hacker trick is to drop a USB drive in a public area, then count on the curiosity of passersby to do the rest. When a facility employee plugs the USB drive into his work computer to identify the owner of the device, the drive automatically installs hidden rootkit software that invites the bad guys in.

Protection: It may sound mundane, but a good deal of cyber security is awareness and education. Hackers are con artists as well as computer scientists, so employees of infrastructure facilities should be taught not to fall for social-engineering tricks.

BBC Mobile | News | Sport | Weather | Travel | TV

NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environm

10 February 2011 Last updated at 15:59 GMT

885 Share

Hackers hit 'at least five oil and gas firms'

Hackers have run rampant through the networks of at least five oil and gas firms for years, reveals a report.

Compiled by security firm McAfee, it details the methods and techniques the hackers used to gain access to the unnamed multinational firms.

Via a combination of con tricks, computer vulnerabilities and weak security controls, the attackers gained access and stole secrets, it says.

The attacks meant hackers had access to some networks for years

The hackers targeted documents about oil exploration and bidding contracts.

Cashing in

Related Stories

Hague: UK is under cyber-attack

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2010/012710-ddos-oil-gas.html

DDoS attacks, network hacks rampant in oil and gas industry, other infrastructure

Oil and gas industry faces the highest rates of victimization, according to Center for Strategic and International

By Ellen Messmer, Network World
January 28, 2010 07:06 AM ET

Massive denial-of-service attacks and "stealthy infiltration" of corporate networks by attackers is a common experience for companies in critical infrastructure sectors, including financial services, energy, water, transportation and telecom, according to a new survey.

Quiz: Separate cyber security fact from fiction

Extortion schemes related to distributed DoS attacks are also rampant, especially in some parts of the world, according to the survey. The report, titled "In the Crossfire – Critical Infrastructure in the Age of Cyber-War," was prepared by the Washington, D.C. policy think tank Center for Strategic and International Studies (CSIS). CSIS asked 600 IT and security professionals across seven industry sectors in 14 countries about their practices, attitudes about security, and the security measures they employ.

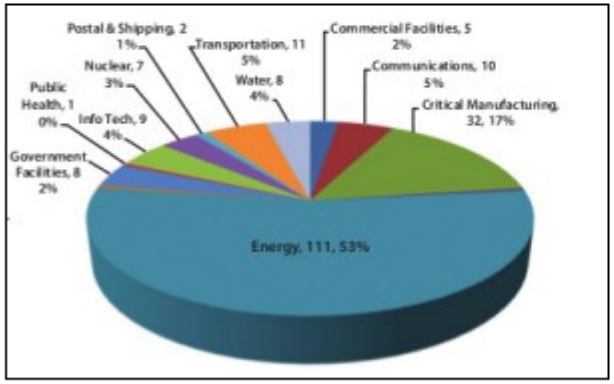
Sponsored by:
Is your business truly collaborative

Intrusiones a ICS

Homeland Security: Hack Attempts On Energy, Manufacturing Way Up in 2013

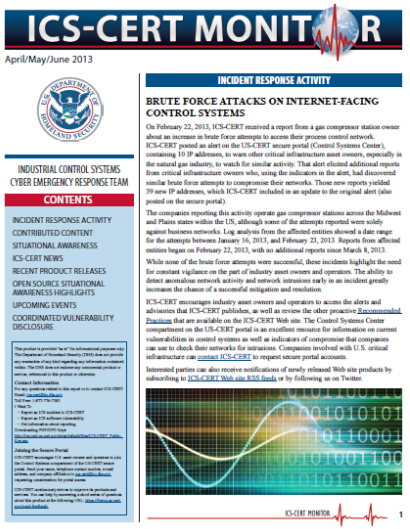
POSTED BY: PAUL JUNE 29, 2013 11:12 0 COMMENTS

Attempted cyber attacks on critical infrastructure in the U.S., including energy and critical manufacturing jumped sharply in the first half of 2013, according to a just-released report from the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT).



ICS-CERT said that cyber incidents across all critical infrastructure in the U.S. are on pace to double in 2013. The agency has responded to 200 such incidents so far in fiscal year 2013 (October of 2012 to May of 2013), compared to 198 incidents for all of fiscal year 2012. A majority of those incidents – 53% – were against organizations in the energy sector, ICS-CERT reported.

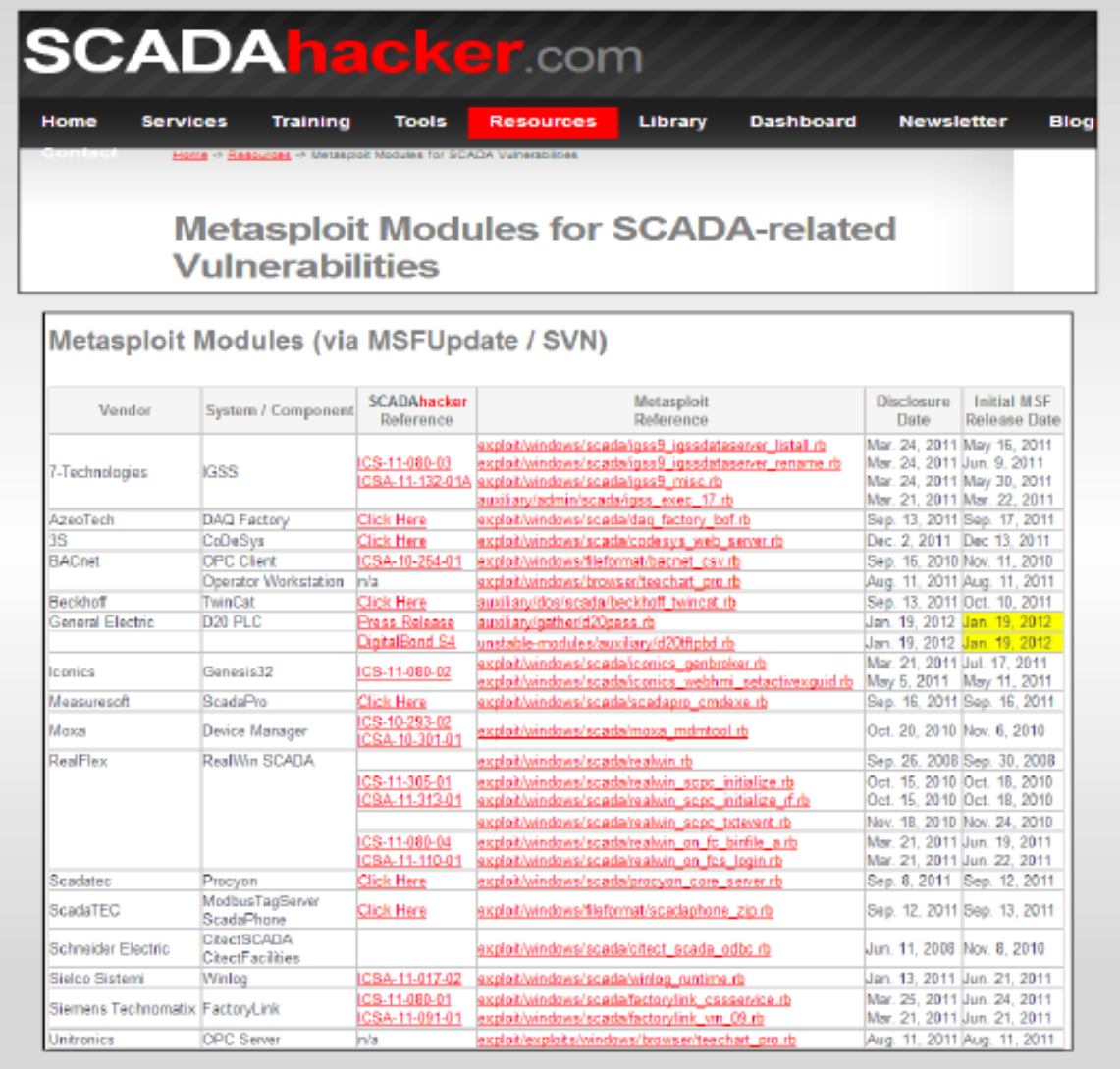
The report is just the latest from DHS about threats to the energy sector. The agency warned energy firms after seeing a sharp jump in attacks



http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

AADECA '14
Mes Nacional del Control Automático

ICS para los chicos



SCADAhacker.com

Home | Services | Training | Tools | Resources | Library | Dashboard | Newsletter | Blog | Contact

Home -> Resources -> Metasploit Modules for SCADA Vulnerabilities

Metasploit Modules for SCADA-related Vulnerabilities

Metasploit Modules (via MSFUpdate / SVN)

Vendor	System / Component	SCADAhacker Reference	Metasploit Reference	Disclosure Date	Initial MSF Release Date
7-Technologies	IGSS	ICS-11-080-03 ICSA-11-132-01A	exploit/windows/scada/igss9_igssdataserver_listall.rb exploit/windows/scada/igss9_igssdataserver_rename.rb exploit/windows/scada/igss9_misc.rb auxiliary/admin/scada/igss_exec_17.rb	Mar. 24, 2011 Mar. 24, 2011 Mar. 24, 2011 Mar. 21, 2011	May 16, 2011 Jun. 9, 2011 May 30, 2011 Mar. 22, 2011
AzeoTech	DAQ Factory	Click Here	exploit/windows/scada/daq_factory_bof.rb	Sep. 13, 2011	Sep. 17, 2011
3S	CoDeSys	Click Here	exploit/windows/scada/codesys_web_server.rb	Dec. 2, 2011	Dec 13, 2011
BACnet	OPC Client	ICSA-10-264-01	exploit/windows/fileformat/bacnet_csv.rb	Sep. 16, 2010	Nov. 11, 2010
	Operator Workstation	n/a	exploit/windows/browser/teechart_pro.rb	Aug. 11, 2011	Aug. 11, 2011
Beckhoff	TwinCat	Click Here	auxiliary/dos/scada/beckhoff_twincat.rb	Sep. 13, 2011	Oct. 10, 2011
General Electric	D20 PLC	Press Release	auxiliary/gather/d20pass.rb	Jan. 19, 2012	Jan. 19, 2012
		DigitalBond S4	unstable-modules/auxiliary/d20ftpbd.rb	Jan. 19, 2012	Jan. 19, 2012
Iconics	Genesis32	ICS-11-080-02	exploit/windows/scada/iconics_genbroker.rb exploit/windows/scada/iconics_webhmi_setactivexguid.rb	Mar. 21, 2011 May 5, 2011	Jul. 17, 2011 May 11, 2011
Measuresoft	ScadaPro	Click Here	exploit/windows/scada/scadapro_cmdexe.rb	Sep. 16, 2011	Sep. 16, 2011
Moxa	Device Manager	ICS-10-293-02 ICSA-10-301-01	exploit/windows/scada/moxa_mdmtool.rb	Oct. 20, 2010	Nov. 6, 2010
RealFlex	RealWin SCADA		exploit/windows/scada/realwin.rb	Sep. 26, 2008	Sep. 30, 2008
		ICS-11-305-01 ICSA-11-313-01	exploit/windows/scada/realwin_scpc_initialize.rb exploit/windows/scada/realwin_scpc_initialize_rf.rb	Oct. 15, 2010 Oct. 15, 2010	Oct. 18, 2010 Oct. 18, 2010
			exploit/windows/scada/realwin_scpc_txtevent.rb	Nov. 18, 2010	Nov. 24, 2010
		ICS-11-080-04 ICSA-11-110-01	exploit/windows/scada/realwin_on_fc_binfile_a.rb exploit/windows/scada/realwin_on_fcs_login.rb	Mar. 21, 2011 Mar. 21, 2011	Jun. 19, 2011 Jun. 22, 2011
Scadatec	Procyon	Click Here	exploit/windows/scada/procyon_core_server.rb	Sep. 8, 2011	Sep. 12, 2011
ScadaTEC	ModbusTagServer ScadaPhone	Click Here	exploit/windows/fileformat/scadaphone_zip.rb	Sep. 12, 2011	Sep. 13, 2011
Schneider Electric	CitectSCADA CitectFacilities		exploit/windows/scada/citect_scada_odbc.rb	Jun. 11, 2008	Nov. 8, 2010
Sielco Sistemi	Winlog	ICSA-11-017-02	exploit/windows/scada/winlog_runtime.rb	Jan. 13, 2011	Jun. 21, 2011
Siemens Technomatix	FactoryLink	ICS-11-080-01 ICSA-11-091-01	exploit/windows/scada/factorylink_csservice.rb exploit/windows/scada/factorylink_vrn_09.rb	Mar. 25, 2011 Mar. 21, 2011	Jun. 24, 2011 Jun. 21, 2011
Unitronics	OPC Server	n/a	exploit/exploits/windows/browser/teechart_pro.rb	Aug. 11, 2011	Aug. 11, 2011

Estrategias de seguridad

Defensa en profundidad

- Protección del perímetro
  - Firewall, IPS, VPN, AV
  - Host IDS, Host AV
  - DMZ
- Seguridad interna
  - Firewall, IDS, VPN, AV
  - Host IDS, Host AV
  - IEEE P1711 (AGA 12)
  - NAC
  - Scanning
- Monitoreo
- Management

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	DeMilitarized Zone
VPN	Virtual Private Network (cryptographic)
AV	Anti-Virus (anti-malware)
NAC	Network Admission Control

Disponibilidad, integridad y confidencialidad

- La red corporativa requiere CID
  - La confidencialidad es lo que más importa
- Los ICS requieren DIC
  - La disponiblidad e integridad importan más
  - La información de control no necesita de tanta confidencialidad
- Asegurar la disponibilidad es complejo
  - La criptografía no ayuda directamente
  - Debe haber protección contra DOS, Gestión de recursos, QoS y redundancia pero con altos niveles de disponibilidad

La seguridad no debe reducir la disponibilidad!

Los dispositivos de los ICS son frágiles

- Muchas de las implementaciones del stack IP son frágiles
  - Algunos dispositivos de “cuelgan” con un simple ataque de ping o un scanning de puertos
  - Muchos incidentes de seguridad se reportan sobre los ICS cuando personas de sector de IT corren un scanning de vulnerabilidades de forma bien intencionada

- Los dispositivos ICS modernos son mucho más sofisticados
  - Algunos IED incluyen un web server para configuración y monitoreo de status
  - Más lineas de código tienden a más vulnerabilidades
  - Los IED más modernos requieren un sistema de patch management

Sistemas sin patches

- La mayoría de los ICS no aplican patches
  - Particularmente Servidores Windows
  - No hay disponibilidad de patches para versiones viejas de sistemas operativos
- Los patches del SO y aplicaciones pueden “romper” el ICS
  - Los patches de SO son testeados en entornos corporativos
- Patches no certificados pueden invalidar la garantía
- Aplicar patches usualmente requiere hacer un reboot
- Antes de la instalación de un patch:
  - Certificación del vendedor (típicamente una semana)
  - Testing en el laboratorio por el operador
  - Deployment planificado en sistemas menos críticos
  - Paradas programadas (1 o 2 veces al año).

Uso limitado del Anti-Virus local

- Las operaciones de los AV pueden causar fallas en el sistema
  - 3am no es el mejor horario que otro para un scanning full del disco en un sistema que opera 24x7x365
- Los vendedores de ICS recien ahora están comenzando a soportar AV
  - Los AV dependen de la base de firmas que posean (actualización)
  - Las actualizaciones pueden requerir procesos de testing previos
- Uso del criterio de whitelist
  - Enumerar las aplicaciones (procesos) “aprobadas”
- Los AV ven un nuevo mercado: **Symantec Critical System Protection**

Autenticación y autorización pobre

- Muchos ICS tienen mecanismos de autenticación pobres y de autorización muy limitados
- Muchos protocolos utilizan passwords en texto plano (telnet, ftp)
- La mayoría de los dispositivos de ICS no soportan criptografía
- La mayoría de las veces el vendedor deja la password por defecto (escrita en el manual de instalación y conocida)
- Los passwords de los dispositivos son complicados de gestionar de forma adecuada:
  - Usualmente el mismo password es compartido por todo el sistema de ICS y nunca se cambia (o no se puede cambiar)
  - Esto pasa HOY EN DIA!

Bajo nivel de auditoría y logging

- La mayoría de los ICS tienen un nivel muy bajo de auditoría de actividades de seguridad (en varios casos, no existe)
  - Los intentos de intrusión o intrusiones pasan desapercibidos
- Cuando los logs se almacenan, raramente se revisan (solamente en el caso de un incidente)
- No hay monitoreo proactivo
- Estan comenzando a aparecer aspectos regulatorios:
  - SOX
  - ICS-CERT
  - US-CERT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Ontario

NIST
National Institute of Standards and Technology

Uso no apropiado de las Estaciones de Trabajo de los ICS

- La navegación en Internet desde Estaciones de Trabajo HMI pueden infectar el ICS
  - Vulnerabilidades del Browser
  - Vulnerabilidades Java (embebido en el Browser)
  - Downloads
  - Cross-site scripting
  - Spyware

- Envío de correo electrónico desde / hacia los Servidores de Control pueden infectar los ICS
  - Vulnerabilidades en outlook, sendmail, etc.

- Almacenamiento en el disco local pueden causar un “crash” del sistema operativo/aplicación
  - Almacenamiento de videos, música, etc.

Acceso por parte de terceros

- El mantenimiento, programación y soporte muchas veces es realizado por el proveedor.
  - Muchos ICS poseen puertos de mantenimiento abiertos
  - Los equipos infectados de los proveedores pueden afectar nuestro ICS

- Los terceros pueden requerir información sobre el status en tiempo real
  - El acceso de terceros muchas veces no implementa mecanismos de seguridad
  - Los canales de acceso de parte de terceros son una vía de acceso por parte de los intrusos

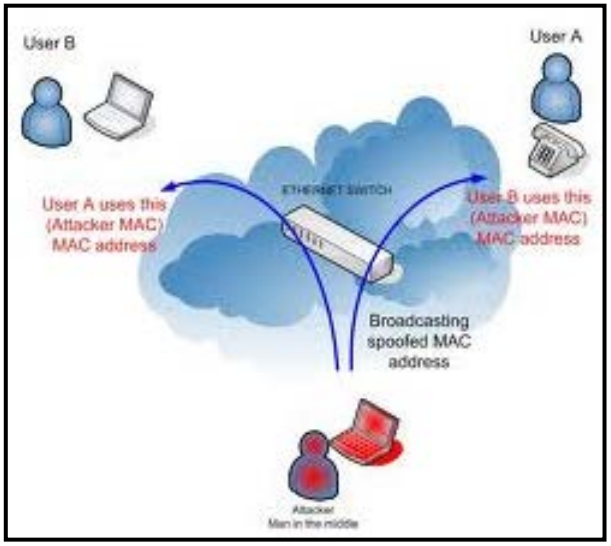
- Terceros pueden incluir: entes reguladores, proveedores de telecomunicaciones, socios comerciales, proveedores de los sistemas, agencias de monitoreo, etc.

El factor humano

- Usualmente las redes de ICS son administradas por ingenieros del área industrial que son distintos del departamento de IT
  - El personal del ICS no son expertos en IT y Seguridad
  - El personal de IT y Seguridad no es experto en ICS

- En la mayoría los casos, el personal que gestiona los ICS es “avanzado en edad tecnológica”.
  - Poca gente joven ingresa en este campo.
  - Hay pocos programas académicos.
  - Mucho conocimiento basado en experiencia y contacto con proveedores.

Estándares y lineamientos de seguridad



ICS CERT

The Industrial Control Systems Cyber Emergency Response Team

ICS-CERT - Windows Internet Explorer
http://ics-cert.us-cert.gov/
Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ICSJWG
TRAINING
FAQ
LEGAL
Control Systems
Home
Calendar
ICSJWG
Information Products
Training
Recommended Practices
Assessments
Standards & References
Related Sites
FAQ
The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.
Learn More
Control Systems Advisories and Reports
Alerts
Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks
Advisories
Advisories provide timely information about current security issues,
On This Page
ICS-CERT Monitor Newsletters
Recently Published
Other Resources
News Feed
Department of Homeland Security
Office of Cybersecurity & Communications
NCCIC
Related Resources
Stop. Think. Connect.
National Institute of Cybersecurity Studies
Report Cyber Risks
Prevent Cyber Intrusions
Inicio

ICS CERT

The Industrial Control Systems Cyber Emergency Response Team

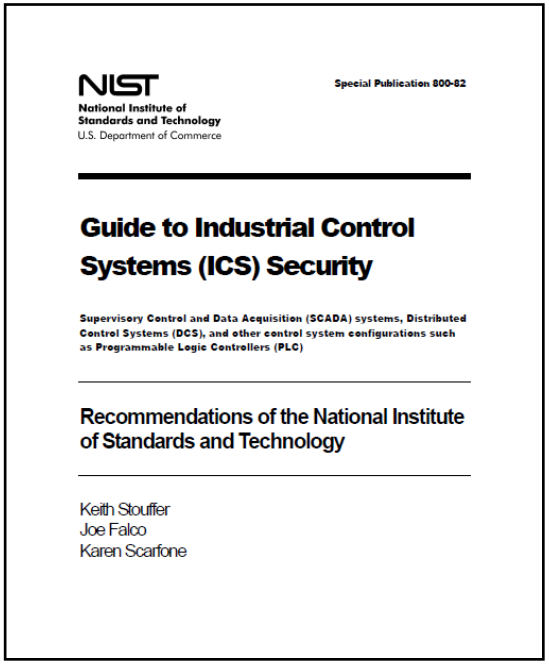
http://ics-cert.us-cert.gov/Standards-and-References

- Cyber Security Policy Planning and Preparation
- Establishing Network Segmentation, Firewalls, and DMZs
- Patch, Password, and Configuration Management
- Control System Cyber Security Training for Engineers, Technicians, Administrators, and Operators
- Establishing and Conducting Asset, Vulnerability, and Risk Assessments
- Control System Security Procurement Requirements Specification
- Placement and Use of IDSs and IPDSs
- Authentication, Authorization, and Access Control For Direct and Remote Connectivity
- Securing Wireless Connections
- Use of VPNs and Encryption in Securing Communications
- Establishing a Secure Topology and Architecture
- Applying and Complying with Security Standards
- Ensuring Security when Modernizing and Upgrading

NIST Special Publication 800-82

NIST Special Publication 800-82
Guide to Industrial Control Systems (ICS) Security
Junio 2011

- Introducción a los sistemas de control industriales (ICS)
- Amenazas y vulnerabilidades de los ICS
- Desarrollo y aplicación de un programa de seguridad para ICS
- Arquitectura de red
- Controles de seguridad de los ICS
- Auditoría de seguridad de ICS


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Recommendations of the National Institute of Standards and Technology

Keith Stouffer
Joe Falco
Karen Scarfone

Nueva versión de Febrero 2015
http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf

SEGURINFO 2015

LIII Congreso y Feria Iberoamericana de Seguridad de la Información

USUARIA

Protección de Infraestructuras Críticas Seguridad en Sistemas de Control Industrial

Presentada por:

Julio César Ardita, CTO CYBSEC

jardita@cybsec.com

CYBSEC Security Systems

SEGURINFO 2015 SEGURINFO 2015 SEGURINFO 2015